IN THE CLAIMS

Please amend claims 13, 21-29, 36 and 43-49, and add new claims 50 and 51.

1. (Original) A method for authentication in a public cryptographic system comprising:

creating a first private key and corresponding first public key;

creating a second private key associated with the first private key and creating a second public key corresponding to the second private key;

outputting the second private key once such that it can be re-created;

outputting the second public key when outputting the first public key; and

using the first private key for authentication.

2. (Original) The method of claim 1, wherein outputting the second public key comprises:

creating at least two shares of the second public key; and

outputting each share once to a different entity.

3. (Original) The method of claim 1, further comprising:

re-creating the second private key; and

using the second private key for authentication.

4. (Original) The method of claim 3, further comprising:

disabling the first private key when the second private key is used for authentication

5. (Original) The method of claim 3, further comprising:

creating a third private key associated with the second private key and creating a third public key corresponding to the third private key; and

outputting the third public key.

6. (Original) The method of claim 5, further comprising:

outputting the third private key once such that it can be re-created; and

re-creating the third private key and using the third private key for authentication.

7. (Original) The method of claim 5, further comprising:

disabling use of the second private key for authentication;

using the third private key for authentication; and

re-creating the second private key and using the second private key for authentication.

8. (Original) The method of claim 3, further comprising:

creating a third private key associated with the second key and creating a third public key corresponding to the third private key;

creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key;

outputting the fourth private key once such that it can be re-created; and

outputting the third and fourth public keys.

9. (Original) The method of claim 8, further comprising:

disabling use of the second private key for authentication; and

using the third private key for authentication.

10. (Original) The method of claim 9, further comprising:

re-creating the fourth private key; and

using the fourth private for authentication.

11. (Original) A method for verification in a public cryptographic system comprising:

receiving a first public key;

receiving a second public key associated with the first public key;

using the first public key for authentication; and

using the second public key for authentication if the first public key fails.

12. (Original) The method of claim 11, further comprising:

receiving a third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

13. (Currently Amended) The method of claim 11, further comprising:

receiving a third public key and a fourth public key ~~associated with the second public key~~, if the first public key fails and if the second public key results in a successful authentication, wherein the third and the fourth public keys are associated with the second key.

14. (Original) Apparatus for authentication in a public cryptographic system comprising:

means for creating a first private key and corresponding first public key;

means for creating a second private key associated with the first private key and creating a second public key corresponding to the second private key;

means for outputting the second private key once such that it can be re-created;

means for outputting the second public key when outputting the first public key; and

means for using the first private key for authentication.

15. (Original) The apparatus of claim 14, wherein means for outputting the second public key comprises:

means for creating at least two shares of the second public key; and

means for outputting each share once to a different entity.

16. (Original) The apparatus of claim 14, further comprising:

means for re-creating the second private key; and

means for using the second private key for authentication.

17. (Original) The apparatus of claim 16, further comprising:

means for creating a third private key associated with the second private key and creating a third public key corresponding to the third private key; and

means for outputting the third public key.

18. (Original) The apparatus of claim 16, further comprising:

means for creating a third private key associated with the second key and creating a third public key corresponding to the third private key;

means for creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key;

means for outputting the fourth private key once such that it can be re-created; and

means for outputting the third and fourth public keys.

19. (Original) Apparatus for verification in a public cryptographic system comprising:

means for receiving a first public key;

means for receiving a second public key associated with the first public key;

means for using the first public key for authentication; and

means for using the second public key for authentication if the first public key fails.

20. (Original) The apparatus of claim 19, further comprising:

means for receiving a third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

21. (Currently Amended) The apparatus of claim 19, further comprising:

means for receiving a third public key and a fourth public key ~~associated with the second public key~~, if the first public key fails and if the second public key results in a successful authentication, wherein the third and fourth public keys are associated with the second public key.

22. (Currently Amended) An article of manufacture comprising a computer system having a public cryptographic system, said article of manufacture comprising a machine readable medium having machine readable code means embodied in said medium ~~A machine readable medium in a public cryptographic system~~ comprising:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to create a first private key and corresponding first public key;

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to create a second private key associated with the first private key and creating a second public key corresponding to the second private key;

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to output the second private key once such that it can be re-created;

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to output the second public key when outputting the first public key; and

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to use the first private key for authentication.

23. (Currently Amended) The article of manufacture ~~medium~~ of claim 22, wherein the machine readable code means to output the second public key comprises:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to create at least two shares of the second public key; and

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to output each share once to a different entity.

24. (Currently Amended) The article of manufacture ~~medium~~ of claim 22, further comprising:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ causing the computer to re-create the second private key; and

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to use the second private key for authentication.

25. (Currently Amended) The article of manufacture ~~medium~~ of claim 24, further comprising:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to disable the first private key by using the second private key for authentication

26. (Currently Amended) An article of manufacture comprising a computer system having a public cryptographic system, said article of manufacture comprising a machine readable medium having machine readable code means embodied in said medium ~~A machine readable medium in a public cryptographic system~~ comprising:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to receive a first public key;

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to receive a second public key associated with the first public key;

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to use the first public key for authentication; and

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to use the second public key for authentication if the first public key fails.

27. (Currently Amended) The article of manufacture ~~medium~~ of claim 26, further comprising:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to receive a third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

28. (Currently Amended) The article of manufacture ~~medium~~ of claim 26, further comprising:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to receive a third public key and a fourth public key, if the first public key fails and if the second public key results in a successful authentication, wherein the third and fourth public keys are associated with the second public key.

29. (Currently Amended) A method for authentication in a public cryptographic system comprising:

creating a private key ~~and corresponding public key with associated system parameter~~, a public key corresponding to the private key, and an associated system parameter;

outputting the system parameter when outputting the public key; and

using the private key for authentication.

30. (Original) The method of claim 29, further comprising:

creating a new private key using a previous private key and the system parameter; and

using the new private key for authentication.

31. (Original) The method of claim 29, further comprising:

creating a counter value indicating the generation of public and private keys; and

outputting the counter value when outputting the public key.

32. (Original) The method of claim 31, further comprising:

creating the new private key using a previous private key and the system parameter based on the counter value; and

using the new private key for authentication.

33. (Original) A method for verification in a public cryptographic system comprising:

receiving a public key;

receiving a system parameter associated with the public key;

authenticating using the public key; and

generating a new public key and authenticating using the new public key, if a previous public key fails, the new public key being derived from the previous public key and the system parameter.

34. (Original) The method of claim 33, wherein generating the new public key comprises:

using a number of powers of the previous public key for authentication; and

accepting one that works as the new public key.

35. (Original) The method of claim 33, further comprising

receiving a counter value indicating the generation of private and public keys; and

generating the new public key using the previous public key and the system parameter based on the counter value.

36. (Currently Amended) Apparatus for authentication in a public cryptographic system comprising:

means for creating a private key ~~and corresponding public key with associated system parameter~~, a public key corresponding to the private key, and an associated system parameter;

means for outputting the system parameter when outputting the public key; and

means for using the private key for authentication.

37. (Original) The apparatus of claim 36, further comprising:

means for creating a new private key using a previous private key and the system parameter.

38. (Original) The apparatus of claim 36, further comprising:

means for creating a counter value indicating the generation of public and private keys; and

means for outputting the counter value when outputting the public key.

39. (Original) The apparatus of claim 38, further comprising:

means for creating a new private key using a previous private key and the system parameter based on the counter value.

40. (Original) Apparatus for verification in a public cryptographic system comprising:

means for receiving a public key;

means for receiving a system parameter associated with the public key;

means for authenticating using the public key; and

means for generating a new public key and authenticating using the new public key, if a previous public key fails, the new public key being derived from the previous public key and the system parameter.

41. (Original) The apparatus of claim 40, wherein generating the new public key comprises:

means for using a number of powers of the previous public key for authentication; and

means for accepting one that works as the new public key.

42. (Original) The apparatus of claim 40, further comprising

means for receiving a counter value indicating the generation of private and public keys; and

means for generating the new public key using the previous public key and the system parameter based on the counter value.

43. (Currently Amended) An article of manufacture comprising a computer system having a public cryptographic system, said article of manufacture comprising a machine readable medium having machine readable code means embodied in said medium ~~A machine readable medium in a public cryptographic system~~ comprising:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to create a private key, a public key corresponding to the private key, and an associated system parameter;

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to output the system parameter when outputting the public key; and

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to use the private key for authentication.

44. (Currently Amended) The article of manufacture ~~medium~~ of claim 43, further comprising:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to create a new private key using a previous private key and the system parameter.

45. (Currently Amended) The article of manufacture ~~medium~~ of claim 43, further comprising:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to create a counter value indicating the generation of public and private keys; and

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to output the counter value when outputting the public key.

46. (Currently Amended) The article of manufacture ~~medium~~ of claim 45, further comprising:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to create a new private key using a previous private key and the system parameter based on the counter value, if the previous private key is not active.

47. (Currently Amended) An article of manufacture comprising a computer system having a public cryptographic system, said article of manufacture comprising a machine readable medium having machine readable code means embodied in said medium ~~A machine readable medium in a public cryptographic system~~ comprising:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to receive a public key;

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to receive a system parameter associated with the public key;

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to authenticate using the public key;

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to generate a new public key and authenticating using the new public key, if a previous public key fails, the new public key being derived from the previous public key and the system parameter.

48. (Currently Amended) The article of manufacture ~~medium~~ of claim 47, wherein the machine readable code to generate the new public key comprises:

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to use a number of powers of the previous public key for authentication; and

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to accept one that works as the new public key.

49. (Currently Amended) The article of manufacture ~~medium~~ of claim 47, further comprising

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to receive a counter value indicating the generation of private and public keys; and

machine readable code means embodied in said machine readable medium ~~a set of code segments~~ for causing the computer to generate the new public key using the previous public key and the system parameter based on the counter value.

50. (New) Apparatus used for authentication comprising:

a processor configured to generate a first private key and corresponding first public key, the processor configured to generate a second private key associated with the first private key and to create a second public key corresponding to the second private key;

a storage medium coupled to the processor, configured to store the first private key; and

a transmitter coupled to the processor, configured to output the second private key once such that it can be re-created and to output the second public key when outputting the first public key;

wherein the processor uses the first private key for authentication.

51. (New) Apparatus used for verification comprising:

a receiver configured to receive a first public key and to receive a second public key associated with the first public key;

a storage medium coupled to the receiver, configured to store the first and second public keys; and

a processor coupled to the receiver, configured to use the first public key for authentication, the processor configured to use the second public key for authentication if the first public key fails.